

Comprendre le fonctionnement WiFi - 802.11

Information :

On va mettre le PC (Windows et Linux), on va étudier l'environnement WiFi, en particulier avec un point d'accès sur raccorder sur l'établissement.

Le schéma

Matériel : Un switch, Un PA, des PCs

Logiciels :

Logiciel SolarWinds TFTP server

Logiciel Mib browser

Logiciel Analyseur Wireshark

Logiciel putty

Configuration Aironet voir les annexes.

Validation + Compte-rendu :

Fournir des hard-copie wireshark à envoyer à alain@margeride.biz



Dans toutes les étapes toutes les configurations seront faites en mode console IOS, voir les annexes.

Etape 1 Etude environnement

Etude environnement

Sous Windows Utiliser le logiciel inSSID

Bouter la machine linux avec la CD

Attention le clavier est querty passer la commande

`loadkeys fr`

Lancer l'interface graphique par `startx`.

Lancer un terminal, taper

`setxkbmap fr`

Depuis l'interface graphique (internet puis Wicd Network Manager) se connecter

Puis lancer un scan par la commande :

`iwlist wlan0 channel ( Que donne cette commande)`

`iwlist wlan0 scan`

A partir de la vous pouvez utiliser les outils linux pour pouvoir déterminer les différentes cellules

`iwlist wlan0 scan | grep -i cell`

`iwlist wlan0 scan > Scan` le mettre dans le fichier Scan puis Faire une étude de l'environnement avec par exemple :

`awk '/Cell/ || /ESSID/' Scan`

`awk '/Cell/ || /Frequency/ || /ESSID/ || /Authen/ || /Cipher/' Scan`

Ou alors pour une cellule

`sed -n '/Cell 01/,/Cell/{//d;p}' | grep -v Unkno`

Etape 2 Etude de connexion avec votre point d'accès

Faire Addressage.

A faire valider par le formateur

Après reset configurer Aironet en mode ligne de commande et invalider l'accès web pour des problèmes de sécurité et d'efficacité

Le configurer , en mode authentification Open, SSID votre prénom.

Configurer les postes, puis vérifier l'interopération PA.

Puis vérifier l'accessibilité du poste windows.

Depuis la machine linux - Les tests

Depuis l'interface graphique (internet puis Wicd Network Manager) se connecter

Puis lancer un scan par la commande :

```
iwlist wlan0 channel ( Que donne cette commande)
```

```
iwlist wlan0 scan
```

A partir de la vous pouvez utiliser les outils linux pour pouvoir déterminer les différentes cellules

```
iwlist wlan0 scan | grep -i cell
```

iwlist wlan0 scan > Scan le mettre dans le fichier Scan puis Faire une étude de l'environnement avec par exemple :

```
awk '/Cell/ || /ESSID/' Scan
```

```
awk '/Cell/ || /Frequency/ || /ESSID/ || /Authen/ || /Cipher/' Scan
```

Ou alors pour une cellule

```
sed -n '/Cell 01/,/Cell/{//d;p}' | grep -v Unkno
```

Noter le channel de votre point d'accès.

Vous allez scanner le comportement d'une autre station qui se connecte.

Pour cela passer les commandes :

```
ifconfig wlan0 down
```

```
iwconfig wlan0 mode monitor channel n (n celui que vous avez déterminé)
```

```
ifconfig wlan0 up
```

wireshark

Puis dans l'interface wlan0

On mettra des filtres du type eap or aeapol (connecter le pc windows puis deconnecter puis reconnecter),

Pour faire le tour des filtres possible aller dans : Expression, puis dans IEEE 802.11 - IEEE 802.11 wireless LAN, on pourra exemple voir l'ensemble des possibilité pour :

Faire du filtrage en utilisant par exemple wlan.fc.type_subtype == (Regarder par exemple les différents type de trame 802.11).

Etape 3

Après reset configurer l'aironet en mode authentification WAP, SSID votre nom .
Faire les mêmes vérifications windows et linux.

Pour Linux on procedera différament :

Depuis la machine linux, rebooter

Les tests

Depuis l'interface graphique (internet puis Wicd Network Manager) se connecter

Puis lancer un scan par la commande :

```
iwlist wlan0 channel ( Que donne cette commande)
```

```
iwlist wlan0 scan
```

Puis lancer

```
airmon-ng start wlan0
```

wireshark (verifier les interface il a créer une interface mon0 c'est celle qu'il faut sniffer)

Il est demande de mettre les filtres et de montrer le process de connexion.

Vous pouver dans wireshark montrer la partie connexion on sniffer wlan0, puis en sniffant mon0 puis les deux, on enlevra les trames parasites.

Pour cela dans une autre fenêtre disconnect puis conect dans l'outils :

'Wicd Network Manager'

A l'aide des filtres wireshark faire une étude des trames, à regarder quand vous vous connecter avec la machine linux et la machine windows

Etape 4

Configurer le point d'accès pour pouvoir y accéder en telnet (putty).

Y accéder depuis un PC, la liaison est elle sécurisée ? On fournira un fichier d'analyse de trames.

Configurer le PA pour pouvoir y accéder en SSH (putty)

Y accéder depuis un PC, la liaison est elle sécurisée ? On fournira un fichier analyse de trames

Etape 5

Sauvegarde des IOS du switch et PA en utilisant le serveur TFTP servi.

Etape 6

Configuration SNMP, puis faire un test avec MIB browser

Lire avec le MIB browser les variables contact, location et les interfaces réseaux, faire une étude.

Annexe : Mise en œuvre aironet

- Réinitialisation à faire systématique au début TP, et entre chaque changement de configuration, la procédure:
Couper le courant, puis à la remise du courant appuyer une dizaine de seconde sur le bouton reset (mode)
- Initialisation du point d'accès

```

ap #conf t
ap(config)#no ip domain-lookup
ap(config)#int bvil
ap(config-if)#ip address 192.168.10.10 255.255.255.0
ap(config-if)#no shutdown
ap(config-if)#exit
ap(config)#int f 0
ap(config-if)#ip address 192.168.10.11 255.255.255.0
ap(config-if)#no shutdown
ap(config-if)#exit
ap(config)#exit
ap #show ip interface brief

```

ANNEXE : Configuration de base

```

ap #conf ter
Enter configuration commands, one per line. End with CNTL/Z.
ap(config)#dot11 ssid surf
ap(config-ssid)#guest-mode
ap(config-ssid)#authentication open
ap(config-ssid)#exit
ap(config)#interface dot11Radio 0
ap(config-if)#ssid surf
ap(config-if)#no shutdown
*%LINK-5-CHANGED: Interface Dot11Radio0, changed state to reset
*%DOT11-6-FREQ_SCAN: Interface Dot11Radio0, Scanning frequencies for 29 seconds
*%DOT11-6-FREQ_USED: Interface Dot11Radio0, frequency 2437 selected
*%LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*%LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio0, changed state to up
*%DOT11-6-ASSOC: Interface Dot11Radio0, Station 000e.35be.47bf Associated
KEY_MGMT[NONE]
ap#show dot11 associations
802.11 Client Stations on Dot11Radio0:
SSID [surf] :
MAC Address      IP address      Device          Name            Parent          State
000e.35be.47bf 192.168.10.252  unknown        -               self            Assoc
ap#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
ap#copy running-config tftp:
Address or name of remote host []? 192.168.10.252
Destination filename [ap-config]? ap-config-aironet1231G-leplussimple
!!
1227 bytes copied in 1.227 secs (1000 bytes/sec)
ap#

```

ANNEXE : Configuration WPA

```
ap#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
ap(config)#dot11 ssid celeste
ap(config-ssid)#authentication open
ap(config-ssid)#authentication key-management wpa
ap(config-ssid)#wpa-psk ascii margeride
ap(config-ssid)#guest-mode
ap(config-ssid)#exit
ap(config)#interface dot11Radio 0
ap(config-if)#encryption mode ciphers tkip
ap(config-if)#ssid celeste
ap(config-if)#no shutdown
ap(config-if)#
* %LINK-5-CHANGED: Interface Dot11Radio0, changed state to reset
* %DOT11-6-FREQ_SCAN: Interface Dot11Radio0, Scanning frequencies for 19
seconds
* %DOT11-6-FREQ_USED: Interface Dot11Radio0, frequency 2417 selected
* %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
* %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio0, changed state
to up
* %DOT11-7-AUTH_FAILED: Station 000e.35be.47bf Authentication failed
* %DOT11-7-AUTH_FAILED: Station 000e.35be.47bf Authentication failed
* %DOT11-7-AUTH_FAILED: Station 000e.35be.47bf Authentication failed
* %DOT11-6-ASSOC: Interface Dot11Radio0, Station 000e.35be.47bf Associated
KEY_MGMT[WPA PSK]
```

ANNEXE : Configuration SSH et DHCP

```
ap#conf terminal
ap(config)#username hello password 2101
ap(config)#line vty 0 4
ap(config-line)#transport input all
ap(config-line)#login local
ap(config)#line console 0
ap(config-line)#login local
```

Pour changer le password sur enable
ap(config)#enable secret 2101

Validation SSH

```
ap#conf terminal
ap(config)#ip domain name alain
ap(config)#crypto key generate rsa
The name for the keys will be: ap.alain
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]:
% Generating 512 bit RSA keys ...[OK]
ap(config)#
*Mar 1 00:17:45.588: %SSH-5-ENABLED: SSH 1.99 has been enabled
ap(config)#
```

<http://mcsindex.com/>

MCS Index	Number of spatial streams	Modulation (Stream 1/ 2/ 3/ 4)	Coding rate	N _{BPS} (SS)	N _{ES}		N _{SD}		N _{CBPS}		N _{DBPS}		Data Rate (in Mbps) (GI = 800ns)		Data Rate (in Mbps) (GI = 400ns)	
					20MHz	40MHz	20MHz	40MHz	20MHz	40MHz			20MHz	40MHz	20MHz	40MHz
0	1	BPSK	1/2	1	1	1	52	108	52	108			6.5	13.5	7.2	15.0
1	1	QPSK	1/2	2	1	1	52	108	104	216			13.0	27.0	14.4	30.0
2	1	QPSK	3/4	2	1	1	52	108	104	216			19.5	40.5	21.7	45.0
3	1	16-QAM	1/2	4	1	1	52	108	208	432			26.0	54.0	28.9	60.0
4	1	16-QAM	3/4	4	1	1	52	108	208	432			39.0	81.0	43.3	90.0
5	1	64-QAM	2/3	6	1	1	52	108	312	648			52.0	108.0	57.8	120.0
6	1	64-QAM	3/4	6	1	1	52	108	312	648			58.5	121.5	65.0	135.0
7	1	64-QAM	5/6	6	1	1	52	108	312	648			65.0	135.0	72.2	150.0
8	2	BPSK	1/2	1	1	1	52	108	104	216			13.0	27.0	14.4	30.0
9	2	QPSK	1/2	2	1	1	52	108	208	432			26.0	54.0	28.9	60.0
10	2	QPSK	3/4	2	1	1	52	108	208	432			39.0	81.0	43.3	90.0
11	2	16-QAM	1/2	4	1	1	52	108	416	864			52.0	108.0	57.8	120.0
12	2	16-QAM	3/4	4	1	1	52	108	416	864			78.0	162.0	86.7	180.0
13	2	64-QAM	2/3	6	1	1	52	108	624	1296			104.0	216.0	115.6	240.0
14	2	64-QAM	3/4	6	1	1	52	108	624	1296			117.0	243.0	130.3	270.0
15	2	64-QAM	5/6	6	1	1	52	108	624	1296			130.0	270.0	144.4	300.0
16	3	BPSK	1/2	1	1	1	52	108	156	324			19.5	40.5	21.7	45.0
17	3	QPSK	1/2	2	1	1	52	108	312	648			39.0	81.0	43.3	90.0
18	3	QPSK	3/4	2	1	1	52	108	312	648			58.5	121.5	65.0	135.0
19	3	16-QAM	1/2	4	1	1	52	108	624	1296			78.0	162.0	86.7	180.0
20	3	16-QAM	3/4	4	1	1	52	108	624	1296			117.0	243.0	130.0	270.0
21	3	64-QAM	2/3	6	1	2	52	108	936	1944			156.0	324.0	173.3	360.0
22	3	64-QAM	3/4	6	1	2	52	108	936	1944			175.5	364.5	195.0	405.0
23	3	64-QAM	5/6	6	1	2	52	108	936	1944			195.0	405.0	216.7	450.0
24	4	BPSK	1/2	1	1	1	52	108	208	432			26.0	54.0	28.9	60.0
25	4	QPSK	1/2	2	1	1	52	108	416	864			52.0	108.0	57.8	120.0
26	4	QPSK	3/4	2	1	1	52	108	416	864			78.0	162.0	86.7	180.0
27	4	16-QAM	1/2	4	1	1	52	108	832	1728			104.0	216.0	115.6	240.0
28	4	16-QAM	3/4	4	1	2	52	108	832	1728			156.0	324.0	173.3	360.0
29	4	64-QAM	2/3	6	1	2	52	108	1248	2592			208.0	432.0	231.1	480.0
30	4	64-QAM	3/4	6	1	2	52	108	1248	2592			234.0	486.0	260.0	540.0
31	4	64-QAM	5/6	6	1	2	52	108	1248	2592			260.0	540.0	288.9	600.0

ANNEXE : Exemple configuration snmp sur AP

```
ap(config)#snmp-server community public RO
ap(config)#snmp-server community private RW
ap(config)#snmp-server host 192.168.100.10 public
ap(config)#snmp-server host 192.168.100.10 private
ap(config)#snmp-server enable traps
ap(config)#snmp-server contact Bond
ap(config)#snmp-server location mI6
```

Lire avec le MIB browser les variables contact, location et les interfaces réseaux, faire une étude.

Feuille de validation

Date:

Membre du group :

Si ok le responsable TP signe à chaque étape validée

Etape 1

Etape 2

Etape 3

Etape 4

Etape 5

Etape 6

Etape 7

Etape 8